Técnico en Redes y Comunicaciones para Computadores

4

TODO SOBRE:

Windows NT

Novell 5.0

Intranet

Hardware de Redes

Proyecto Completo: Cableado Estructurado

En este fascículo:

Software

- Conceptos Básicos de Controladores de Dominio.
- Relaciones entre Estaciones de Trabajo y Dominios.
- Plan de Cuentas.
- Integración de Windows NT con otros Sistemas Operativos de redes.

Hardware

- Topología de Redes II
- Método de Acceso.
- Comunicación Inter Redes.
- Protocolos de Bajo Nivel.

Argentina $3,30 - México $ 27 - Chile $1.350 - Colombia $4.500 - Venezuela Bs. 1850
Perú S/7,00 - Uruguay - Panamá B/2,50 - Bolivia - Guatemala

9 789589 643037 00004

CODESIS
COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Técnico en Redes y Comunicaciones para Computadores

Realizado y Editado por:

CODESIS
COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Avenida 22 No. 40 - 77 Of. 302
Telefax: 337 7052 - 335 0481
244 5387 - 335 0767
368 7180 - 269 4037
Santafé dce Bogotá, D.C. - Colombia
E-mail:
codesis@multi.net.co
www.codesis.com.co

Esta es una obra editorial
Realizada y Editada por:
CODESIS LTDA.
Comercializadora Editorial
y Sistemas Ltda.

Presidente: Jesús Rueda S.
Gerente General: Gustavo Rueda S.
Subgerente General: Germán Salazar D.
Autores:
Hardware/Software/Comunicaciones:
Gustavo Rueda S.
Jesús Rueda S.
Dirección Técnica y Proyectos
Gustavo Rueda S.
Diseño y Programación:
Yamile Assis R.
Miguel I. Morales V.
Juan D. García (CD-Roms)
Junta Administrativa:
Gloria Rueda S.
Norberto Cárdenas R.

© CODESIS LTDA., 2.000
Santafé de Bogotá - Colombia

Todos los derechos reservados, prohibida su reproducción total o parcial por cualquier medio sin permiso escrito del editor.

ISBN: 958-96430-3-5

Impreso en Colombia.
Printed In Colombia
Impreso por: Printer Colombiana s.a

La obra **TECNICO EN REDES Y COMUNICACIONES PARA COMPUTADOR** de **CODESIS LTDA., Comercializadora Editorial y Sistemas Ltda.** Es una publicación de aparición semanal en forma de 40 (cuarenta) fascículos, encuadernables en 4 (cuatro) volúmenes.
Cada fascículo consta de 4 páginas cubiertas y 20 páginas de contenido a todo color, que se dividen en Software y Hardware.
Las páginas de cada sección son encuadernables por separado, por esta razón al formar los volúmenes, debe cuidarse de desprender previamente, de todos los fascículos, las páginas de cada uno de los temas (Software y Hardware).
Durante la publicación de los fascículos, se pondrán a la venta las tapas de los 4 volúmenes de la obra para su respectiva encuadernación.
En la contraportada interior (tercera de portada) de cada fascículo, encontrará un test de **20** preguntas de evaluación de los temas tratados en él, para establecer los logros obtenidos y el nivel de aprendizaje alcanzado. Si desea obtener el título que lo acredita como **TECNICO EN REDES Y COMUNICACIONES PARA COMPUTADOR**, deberá enviarlos debidamente resueltos los 40 test (se pueden enviar uno a uno ó todos los 40 al final de la obra) a nuestra dirección en Santafé de Bogotá o nuestro e-mail: codesis@multi.net.co; luego de la respectiva calificación y aprobación podrá obtener el **DIPLOMA**.

CODESIS LTDA., Garantiza la total publicación de la obra, el suministro de las tapas necesarias para su encuadernación y el servicio de números atrasados hasta después de un año de terminada la circulación del último fascículo. Garantiza también la calidad del presente material, así como la entrega de los CD-Rom durante el desarrollo de la obra. Sin embargo no se responsabiliza por posibles daños en equipos, hardware, software o información causados por la manipulación errónea de éstos o por defectos en su fabricación o utilización.

CODESIS LTDA., No asume ninguna responsabilidad por daños y/o perjuicios que pudieran resultar de la información contenida en esta obra.
La utilización de cualquier término en esta colección no debe interpretarse como usurpación ilegal de ninguna marca registrada.

MARCAS REGISTRADAS:
COMPAQ (Compaq Computer Corporation) - IBM (international Busines Machines) - MS-DOS/Windows 3.1/Windows 95/Windows 98/Windows NT Server/Windows NT Workstation/Lan Manager (Microsoft Corporation) - Netware y Novell (Novell) - 3Com/Cardfacts/Etherlink/Linkbuilder/Parallel Tasking/Netbuilder/Lanplex/Acces Builder/SmartAgent/Superstack/FDDILink/ATMLink/Autolint (3Com Corporation) - Netscape Navigator (Netscape Comunication Corporation) - Apple y Macintosh (Apple Computer Inc.) -0 HP y Laserjet (Hewlett Packard) - Epson (Epson Corporation) - SMC (Standar Macrosystem Corporation)

DISTRIBUCION INTERNACIONAL:

Colombia:	DISTRIBUIDORAS UNIDAS S.A.	Teléfono:413 9300 (Santafé de Bogotá)
México:	DISTRIBUIDORA INTERMEX S.A.	Teléfono:230 9500 (México D.F.)
Venezuela:	DISTRIBUIDORA CONTINENTAL	Teléfono:4064 111 (Caracas)
Argentina:	DISTRIBUIDORA BERTRAN (Interior)	Teléfono:43031870(Buenos Aires)
	DIST. VACCARO SÁNCHEZ (Capital)	Teléfono:43031871(Buenos Aires)
Chile:	DISTRIBUIDORA ALFA S.A.	Teléfono:5255599 (Santiago)
Ecuador:	DISTRIBUIDORA DE LOS ANDES S.A.	Teléfono:271 644 (Guayaquil)
Perú:	DISTRIBUIDORA BOLIVARIANA S.A.	Teléfonos: 441 3160 (Lima)
Panamá:	DISTRIBUIDORA PANAMEX S.A.	Teléfono: 221 7015 (Panamá)

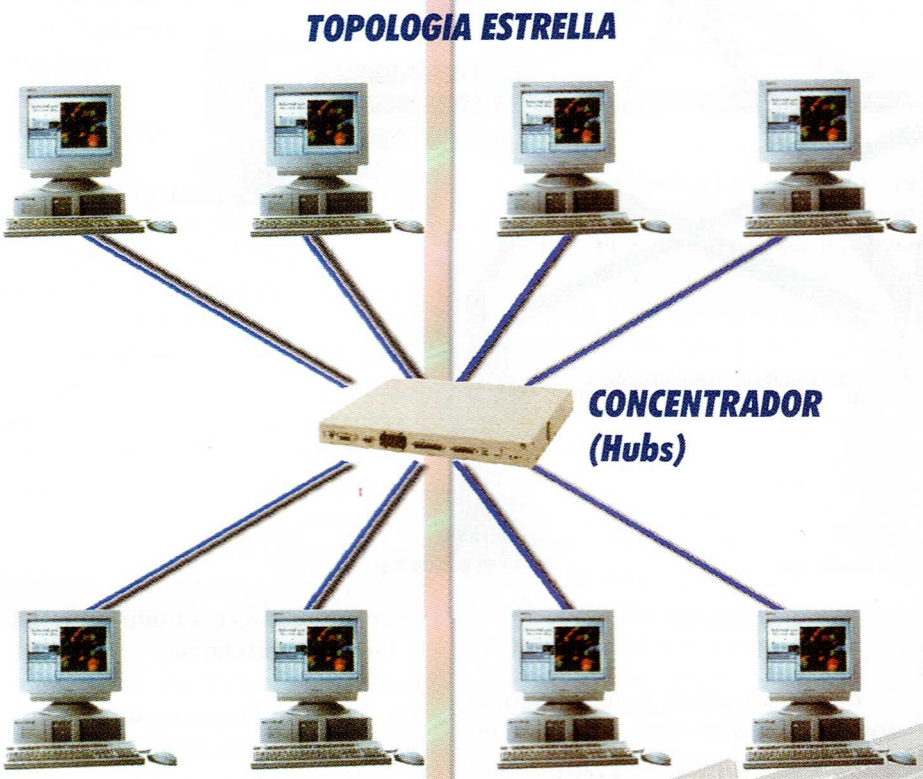
REALIZADO Y EDITADO POR:

CODESIS
COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Avenida 22 No. 40 - 77 Of. 302
Teléfonos: 337 7052 - 335 0481 - 244 5387
Santafé de Bogotá, D.C. - Colombia
E-mail: codesis@multi.net.co

Tropología Estrella.

Es otra de las tres principales topologías. La red se une en un único punto, normalmente con control centralizado, como un concentrador de cableado. Todas las estaciones se conectan al concentrador y las señales son distribuidas a todas las estaciones específicas del concentrador.



Árbol.

Esta estructura de red se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

Trama.

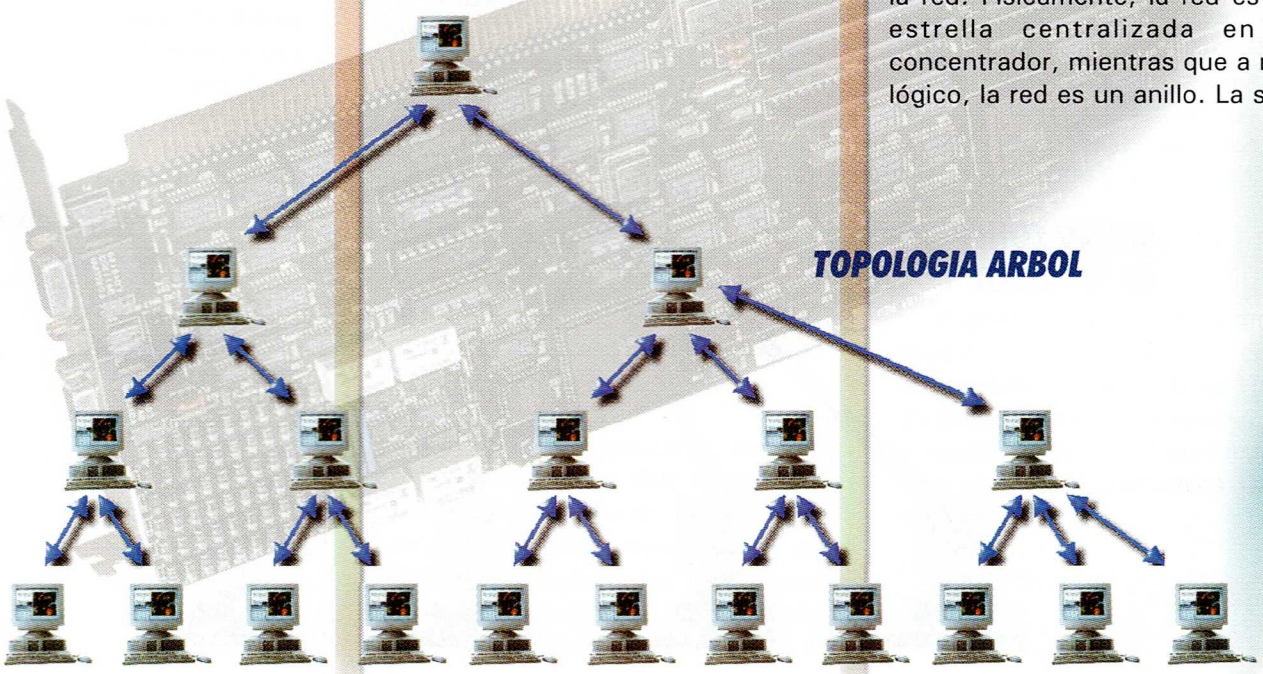
Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (LAN). Las estaciones de trabajo están conectadas cada una con todas las demás.

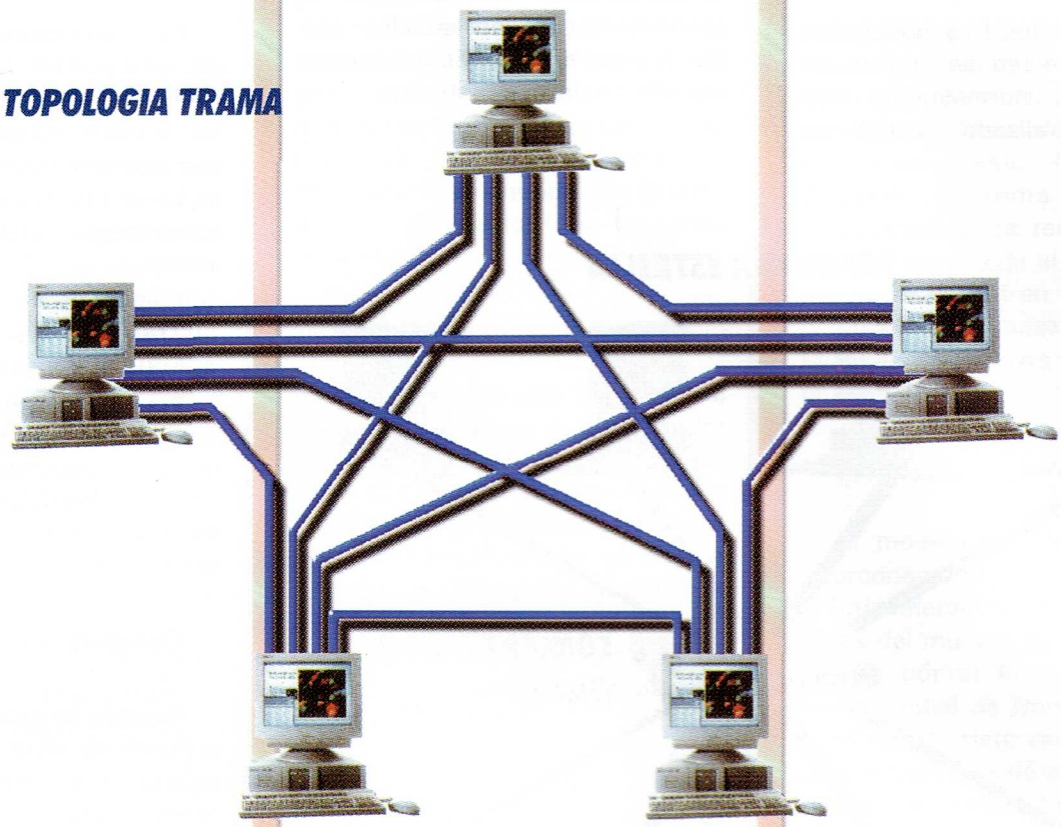
Combinadas.

Cuando se estudia la red desde el punto de vista puramente físico aparecen las topologías combinadas.

Anillo en estrella.

Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo. La señal



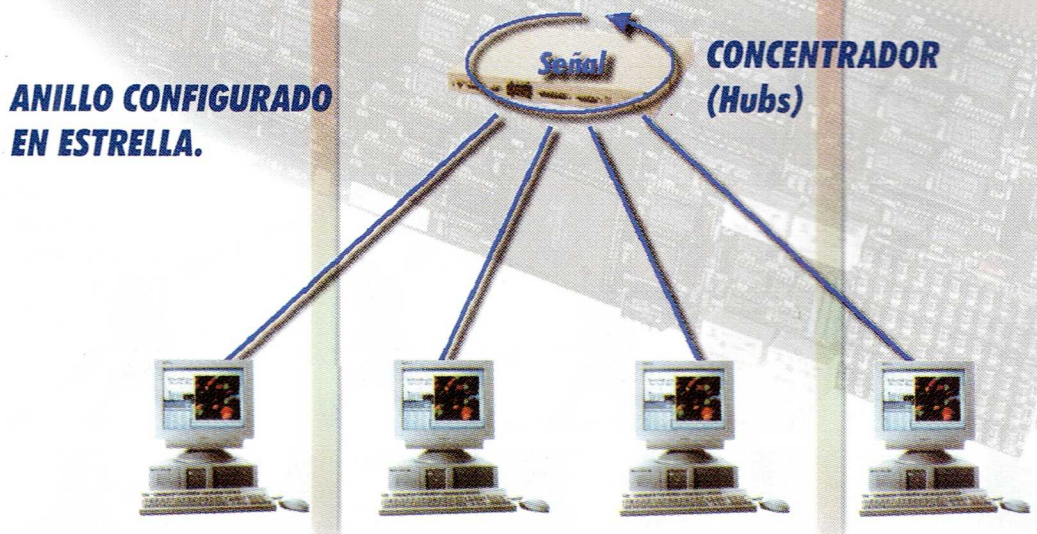


pasa de una estación a otra en círculo. La topología física en la que las estaciones parten de los concentradores o Hubs. El Tokenn Ring 802.5 de IEEE es la principal topología de estrella/anillo.

Bus en estrella.

El fin es igual a la topología anterior. En este caso la red es un bus que se cablea físicamente como una estrella por medio de concentradores. Una red que tiene grupos de estaciones configuradas en estrella conectada con tramos largos de bus lineal.

NOTA: Si todas las estaciones se encuentran en fila (como en un salón de clases o a lo largo de un pasillo en un edificio de oficinas), es una topología de Bus la cual utiliza



CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

cable coaxial (Ethernet).El 10 baseT de Ethernet es una topología de estrella /bus que utiliza cable par trenzado para conectar estaciones al concentrador central, la interrupción en un cable sólo afecta la estación conectada al segmento del cable. En una red de red de bus Ethernet y una red de estrella /bus Ethernet, las señales de las estaciones son difundidas a todas las estaciones del mismo segmento.

A continuación listamos las diferentes formas de topología y su longitud máxima de los segmentos de cada una .

InterRedes.

Un nuevo concepto que ha surgido a partir de todos estos esquemas es el concepto de InterRedes, que es el hecho de vincular redes como si se vincularan estaciones.

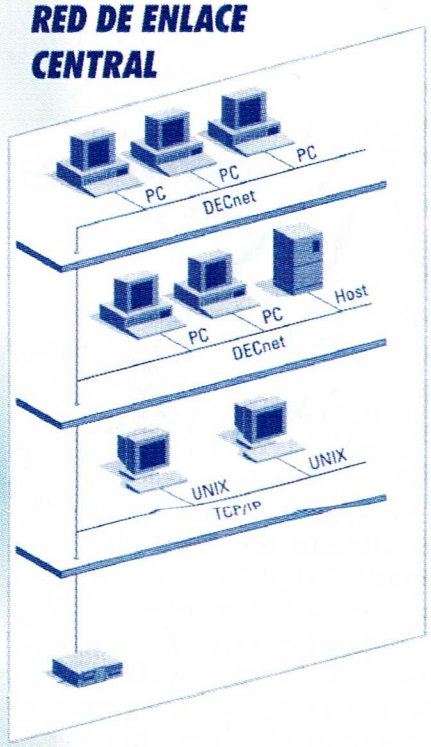
Este concepto, y las ideas que de este surgen, hace brotar un nuevo tipo especial de dispositivo que es un vinculador para interconectar redes entre sí (*la tecnología de Internet está basada en el concepto de InterRedes*), el dispositivo en cuestión se denomina "dispositivo de interconexión". Es decir, lo que se conecta son redes locales de trabajo.

Una red de interconexión consta de LANS de diferentes departamentos o sitios que se interconectan con Bridges o routers.

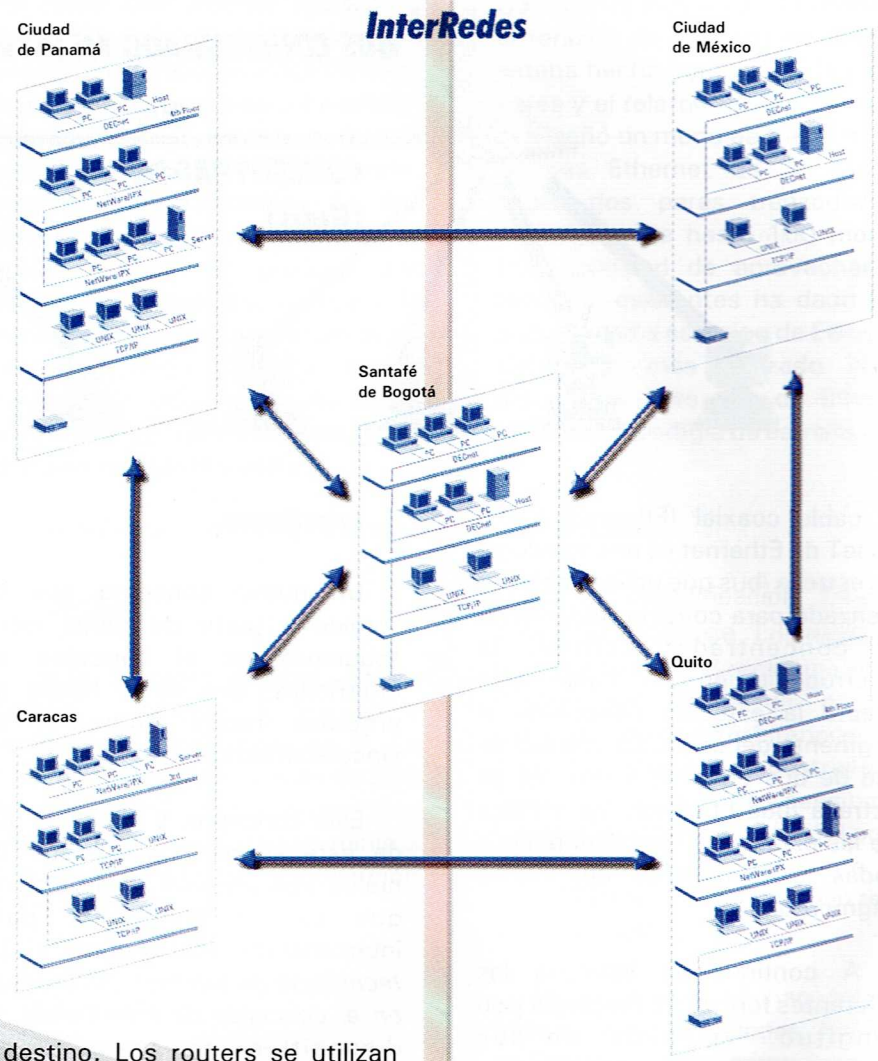
Un enlace central es utilizado a menudo en los entornos locales, como un edificio. Los servicios públicos como las empresas de servicios telefónicos proporcionan enlaces de área metropolitana o de gran alcance las tres topologías.

TOPOLOGIA DE RED	LONGITUD SEGMENTO MÁXIMO
Ethernet de cable fino (Bus)	185 Mts (607 pies).
Ethernet de par trenzado (Estrella, Bus)	100 Mts (330 pies).
Token Ring de par trenzado (Estrella, Anillo)	100 Mts (330 pies).
ARCNET Coaxial (Estrella)	609 Mts (2.000 pies).
ARCNET Coaxial (Bus)	305 Mts (1.000 pies).
ARCNET de par trenzado (Estrella)	122 Mts (400 pies).
ARCNET de par trenzado (Bus)	122 Mts (400 pies).

RED DE ENLACE CENTRAL



InterRedes



Para estos tipos de redes son:

- Red de enlace central
- Red malla
- Red Estrella jerárquica

Red de enlace central.

Una red de enlace central se encuentra generalmente en los entornos de oficina o campos, en los que las redes de los pisos de un edificio se interconectan sobre los cables centrales. Los bridges y los routers gestionan el tráfico entre los segmentos de red conectados.

Red Malla.

Es parecida a la red trama, pero ésta se efectúa a través de redes WAN, una red malla contiene múltiples caminos si un a camino falla o está congestionado el trafico, un paquete puede utilizar un camino diferente hacia el destino. Los routers se utilizan para interconectar las redes separadas.

Estrella Jerárquica.

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica. Los concentradores configurados en estrellas por pisos o por departamentos están unidos por un concentrador central que maneja el tráfico de la interconexión de la red.

Métodos de Acceso.

Una de las características más importantes de las LANS es que son redes compartidas en las que están conectadas varias estaciones, pero solo una estación de trabajo puede efectuar transmisión en un momento determinado. El método de acceso al cable define el protocolo de comunicación que una estación de trabajo debe seguir para realizar una transmisión en un cable compartido.

Los métodos de acceso al cable primario son:

- La detección de la portadora
- El paso de testigo

Estos dos métodos definen

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Promoción y Degradación de Controladores de Dominio.

Además del controlador principal del dominio **(PDC)**, también debe tener uno o más controladores de reserva **(BDC)** en cada dominio.

Si el PDC deja de estar disponible, puede promoverse un BDC, para que sea el controlador principal del dominio, continuando así el funcionamiento del dominio.

En esta situación, son aplicables las siguientes reglas:

- Cuando se promueve un BDC a PDC, se duplica una copia actualizada de la base de datos de directorio del dominio desde el antiguo PDC al nuevo, y el antiguo PDC se degrada a BDC.

- Si se ha promocionado un BDC a PDC mientras el PDC no se encontraba disponible (por ejemplo, mientras se estaba reparando), al volver a funcionar el antiguo PDC, es necesario degradarlo a BDC. Si no se hace así, el PDC actual no podrá ejecutar el servicio Inicio de sesión, no participará en la autentificación de inicios de sesión de usuarios y su icono en la ventana del Administrador de servidores aparecerá atenuado.

Normalmente, cuando se promueve un BDC a PDC, el sistema degrada automáticamente el PDC anterior a BDC. Sin embargo, si el Administrador de servidores no puede localizar el PDC, no lo degrada y el usuario recibe un mensaje que indica tal situación. El usuario puede elegir continuar sin degradar el PDC o esperar hasta que se pueda degradar.

Sincronización de la Base de Datos de Directorio.

Windows NT Server se encarga de sincronizar automáticamente la base de datos de directorio. Basándose en los valores del registro, el PDC envía periódicamente avisos que indican a los BDC que deben solicitarle las modificaciones del directorio. Estos avisos se intercalan, para evitar que todos los BDC soliciten los cambios al mismo tiempo. Cuando un BDC solicita los cambios, informa al PDC del último cambio que ha recibido. De esta forma el PDC siempre detecta qué BDC precisa cambios. Si un BDC está actualizado, su servicio Inicio de sesión no solicita cambios.

Sincronización Parcial y Total.

Se denomina Sincronización parcial a la duplicación automática y periódica en todos los BDC del dominio teniendo en cuenta solo los cambios realizados en la base de datos de directorio desde la última sincronización Puede utilizar el Administrador de servidores para forzar una sincronización parcial de todos los BDC del dominio. Por ejemplo, si se agrega al dominio un nuevo usuario que precisa con urgencia unos recursos, puede realizarse una sincronización parcial para que la nueva cuenta se agregue a todos los BDC tan pronto como sea posible.

Si es necesario, puede utilizar el Administrador de servidores para forzar manualmente la sincronización parcial de un BDC determinado con el PDC. Por ejemplo, si se deniega el acceso a causa de un problema con la contraseña de la cuenta de equipo del BDC (lo cual provoca mensajes "acceso denegado" en el registro de sucesos), una sincronización parcial del BDC con el PDC resolverá el problema de la contraseña y restablecerá un canal seguro.

Enviar una copia de toda la base de datos de directorio a un BDC se denomina sincronización total. La sincronización total se realiza automáticamente cuando se han eliminado del registro de cambios las modificaciones que aún no han sido duplicadas (como se describió en el ejemplo anterior) y cuando se agrega un nuevo BDC al dominio.

Las opciones predeterminadas del servicio Inicio de sesión para el tiempo entre actualizaciones (cada cinco minutos) y el tamaño del registro de cambios (unos 2.000 cambios) aseguran que la sincronización total no será necesaria en la mayoría de las situaciones de funcionamiento.

La sincronización total a través de un vínculo WAN lleva tiempo y es costosa. Para evitar que se produzca una sincronización total no prevista, puede aumentar el tamaño del registro de cambios.

Sincronización de Controladores de Dominio.

En el Administrador de servidores, el comando de menú **Equipo** permite sincronizar los cambios, dependiendo del tipo de computador seleccionado:

- Cuando está seleccionado el BDC, el comando **Sincronizar el dominio completo** está disponible en el menú **Equipo**. Este comando copia los últimos cambios de la base de datos de directorio del PDC a todos los BDC del dominio. Sincronizar el dominio completo

inicia la sincronización de todos los BDC sin esperar a que finalice la sincronización en curso.

- Cuando está seleccionado un controlador de reserva, en el menú **Equipo** se encuentra disponible el comando **Sincronizar con el controlador principal del dominio**. Este comando copia los últimos cambios de la base de datos de directorio únicamente al BDC seleccionado.

Forma de Agregar, Cambiar el Nombre, Mover y Quitar Equipos de un Dominio.

Un dominio se crea al instalar Windows NT Server en un computador y designándolo como controlador de dominio. Después pueden agregarse otros computadores al dominio.

Para que un computador con Windows NT Workstation o Windows NT Server pueda ser un miembro del dominio y participar en su seguridad, es necesario agregarlo al dominio. Cuando se agrega un computador a un dominio, Windows NT Server crea una cuenta para el computador. Si el computador agregado es un controlador de reserva, solicita una copia de la base de datos de directorio del dominio.

Al quitar de un dominio un computador con Windows NT Workstation o Windows NT Server, se elimina la cuenta para el computador. Para agregar un computador a otro dominio se tiene que crear una nueva cuenta para el computador y luego el computador puede unirse al dominio.

Nota: Para quitar de un dominio un controlador de reserva, tiene que eliminar la cuenta para el computador y volver a instalar Windows NT Server en ese computador, indicando el nuevo dominio.

Agregar una Estación de Trabajo o un Servidor a un Dominio.

Al iniciar una sesión con una cuenta de usuario que posea los derechos de usuario adecuados, se pueden agregar estaciones de trabajo y servidores a los dominios durante la instalación o después de ella.

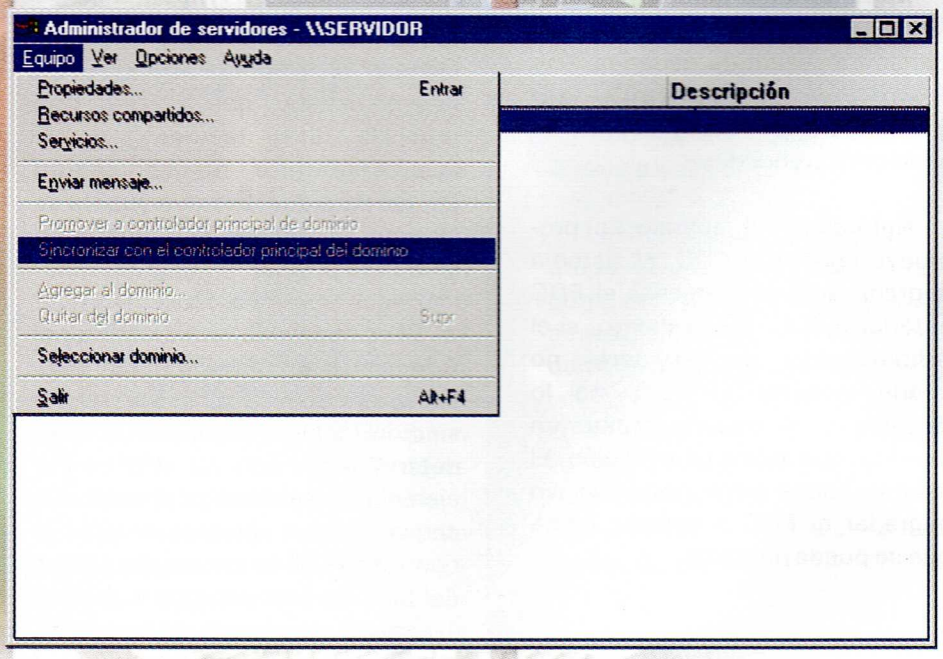
Una vez creado un dominio, un miembro del grupo local Administradores u Operadores de cuentas, puede agregar al dominio un controlador de reserva. El controlador principal del dominio y de reserva sólo se pueden agregar durante la instalación.

No es posible agregar un controlador principal del dominio a un dominio existente.

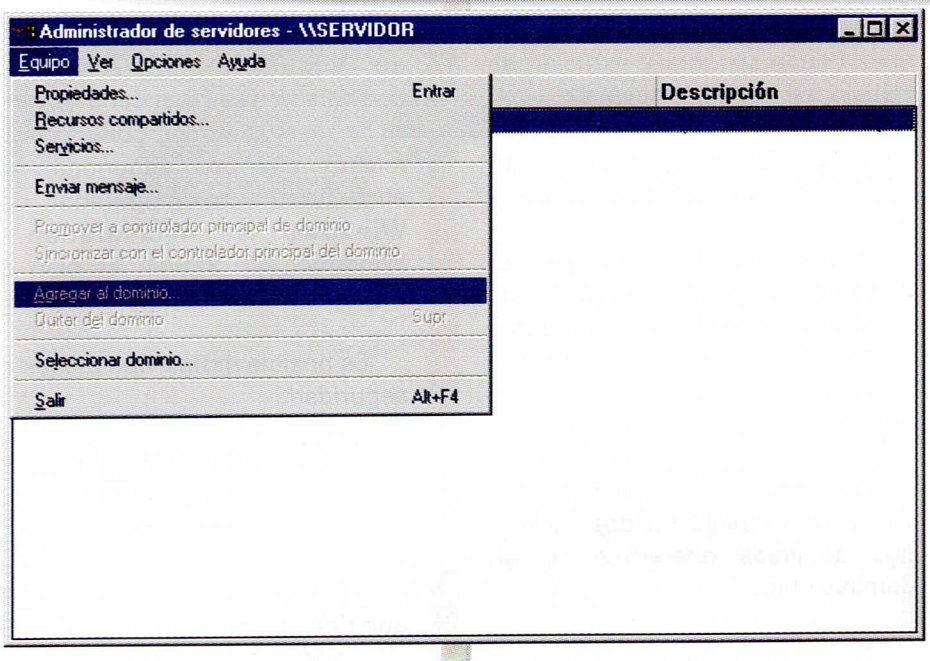
Durante la instalación de Windows NT Server, un miembro del grupo Administradores u Operadores de cuentas o un usuario que tiene el derecho "**Agregar estaciones de trabajo al dominio**" puede agregar al dominio un computador con Windows NT Server como servidor miembro.

- Durante la instalación de Windows NT Workstation, un miembro del grupo Administradores u Operadores de cuentas o un usuario que tenga el derecho "**Agregar estaciones de trabajo al dominio**" puede agregar al dominio un computador con Windows NT Workstation.

Después de la instalación, un miembro del grupo Administradores u Operadores de cuentas o un usuario que tenga el derecho "**Agregar estaciones de trabajo al dominio**" puede agregar al dominio un computador existente con Windows NT Workstation o un servidor miembro, utilizando la opción **Red** en el **Panel de control** del computador que se está agregando.



CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.



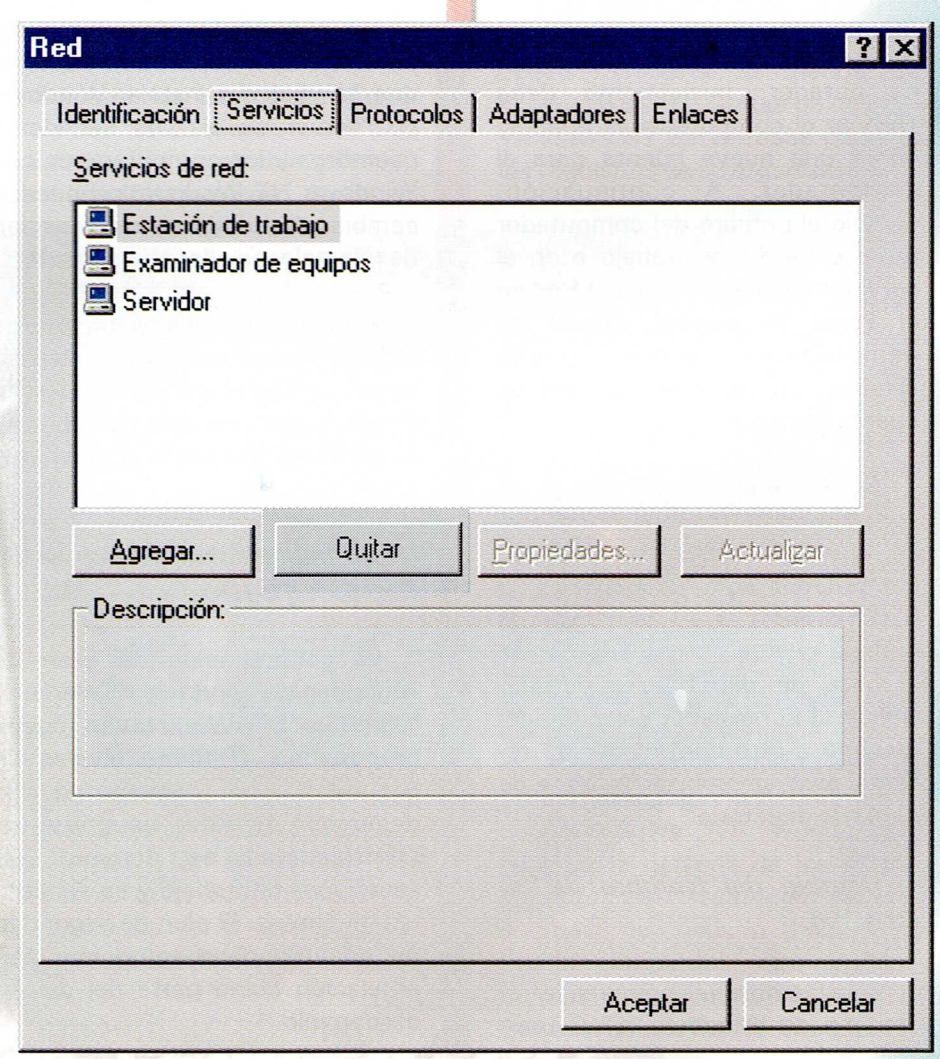
Después de la instalación, un miembro del grupo Administradores u Operadores de cuentas o un usuario que tenga el derecho "**Agregar estaciones de trabajo al dominio**", puede utilizar el comando **Agregar al dominio** en el **Administrador de servidores**, para agregar una cuenta de computador a la base de datos de seguridad del dominio. Así, un usuario de ese computador puede permitirle al computador unirse al dominio, escribiendo el nombre del dominio en la opción **Red** en el **Panel de control** del computador que se está agregando.

Se debe tener cuidado al configurar la seguridad de los nombres de computador que se agreguen. Hasta que el computador se una al dominio, es posible que otro usuario asigne ese nombre a otro computador diferente, uniéndolo después al dominio con la cuenta de computador que se acaba de crear. Si el computador agregado es un controlador de reserva, al unirse al dominio recibe una copia de la base de datos de seguridad del dominio.

Quitar un Computador de un Dominio.

Puede eliminar de un dominio las estaciones de trabajo, controladores de reserva y servidores miembros, pero NO el controlador principal del dominio, hasta que promueva un controlador de reserva a controlador principal.

Al quitar un computador con Windows NT Workstation o un servidor miembro de un dominio de Windows NT Server, se elimina la cuenta para el computador de la base de datos de directorio, por lo que no podrá participar en la seguridad del dominio. Una vez eliminada la cuenta para el computador del dominio, el usuario



del computador debe eliminar el nombre del dominio mediante la opción **Red** en el **Panel de control**. Seguidamente, el usuario puede agregar un nombre de dominio o de grupo de trabajo diferentes.

Para quitar un controlador de reserva de un dominio, es necesario eliminar la cuenta para el computador correspondiente y volver a instalar en ese computador Windows NT Server o Windows NT Workstation, indicando el nuevo dominio. No utilice un controlador de reserva que se ha eliminado de un dominio, hasta que reinstale el sistema operativo.

Cambio del Nombre de Computador de una Estación de Trabajo o de un Servidor.

Para cambiar el nombre de un computador, inicialmente debe agregar el computador al dominio como una nueva cuenta para el computador. A continuación, cambie el nombre del computador en la estación de trabajo o en el servidor mediante la opción **Red** en el **Panel de control**. Desde su computador, después puede eliminar del dominio la antigua cuenta de computador.

Si va a cambiar el nombre de un controlador de reserva, asegúrese de que el nuevo nombre de computador esté reflejado en la base de datos antes de eliminar la antigua cuenta de computador de la base de datos de directorio. Utilice el controlador principal del dominio u otro controlador de reserva para sincronizar la base de datos de directorio.

Cambio del Nombre de un Dominio.

Para cambiar el nombre de un dominio de Windows NT Server, vuelva a escribir el nombre de dominio en cada servidor y estación de trabajo del dominio, después, vuelva a establecer las relaciones de confianza. El identificador de seguridad del dominio (SID) no cambia.

Puede seguir este procedimiento para cambiar el nombre de dominio en todos los computadores dentro de un dominio, pero NO trasladar un controlador de un dominio a otro.

Tampoco puede utilizarlo para dividir un dominio en dos, ni unir dos dominios diferentes en un dominio único.

Traslado de un Computador a otro Dominio.

Un controlador de reserva no puede cambiar de dominio a menos que se vuelva a instalar Windows NT Server en él. Los servidores miembros y los computadores con Windows NT Workstation pueden cambiar de dominio sin necesidad de reinstalar en ellos Windows NT.

Para mover una estación de trabajo o un servidor miembro desde un dominio de Windows NT Server a otro, quite el computador del dominio antiguo y agréguelo al nuevo.

Administración de Planes de Seguridad de Dominio.

La configuración del plan de seguridad de Windows NT Server y Windows NT Workstation puede proporcionar distintos niveles de seguridad con respecto a las acciones de los usuarios en controladores de dominio, en estaciones de trabajo y en servidores miembros. El plan de seguridad de dominio debe estudiarse con antelación como parte del diseño del dominio.

Al administrar dominios, el plan de seguridad se aplica al controlador principal del dominio y al de reserva (todos comparten el mismo plan de seguridad). Al administrar un computador con Windows NT Workstation o Windows NT Server, el plan de seguridad sólo se aplica a él.

Es posible definir tres planes de seguridad:

- El Plan de cuentas controla cómo las cuentas de usuario utilizan las contraseñas.

- El Plan de auditoría controla qué tipos de sucesos se graban en el registro de seguridad (el cual puede examinar con el Visor de sucesos si ha iniciado una sesión como miembro del grupo Administradores).

- El Plan de relaciones de confianza controla en qué dominios se confía y cuáles son los dominios que confían. Este plan no se utiliza en el modelo de dominio único y no está disponible al administrar un computador con Windows NT Workstation o un computador con Windows NT Server como un servidor miembro.

- Un cuarto plan de seguridad, el Plan de derechos de usuario, se aplica a los grupos de usuarios y afecta a las actividades permitidas tanto en las estaciones de trabajo individuales o servidores miembros como en todos los controladores de un dominio.

Configuración del Plan de Contraseñas (cuentas) de Usuario.

El Plan de cuentas controla cómo se deben utilizar las contraseñas en todas las cuentas de usuario de un computador o

dominio y también determina el plan de bloqueo de cuentas.

Entre las restricciones a las contraseñas se encuentran los límites de caducidad, si pueden cambiarse y cuándo debe producirse el cambio, si cada contraseña nueva debe ser distinta de las anteriores y qué longitud puede tener una contraseña.

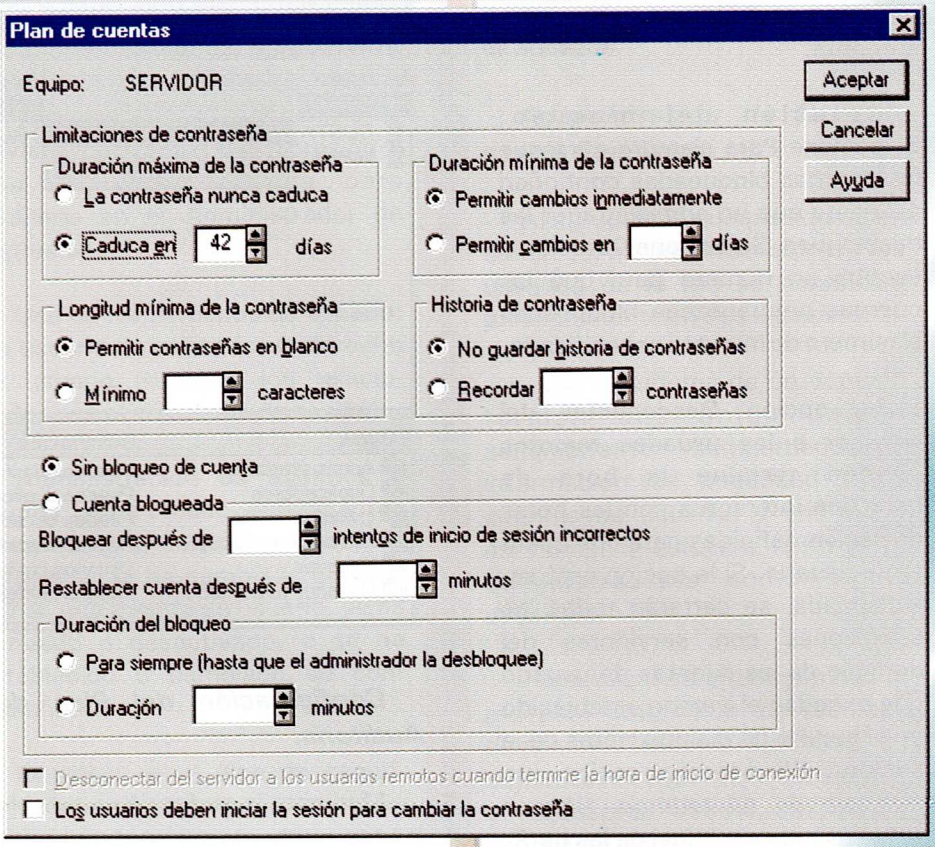
La característica de bloqueo de cuenta permite hacer más seguro a Windows NT Server frente a intrusos que intenten iniciar una sesión probando contraseñas para las cuentas de usuario existentes. Cuando está activado el bloqueo de cuentas, una cuenta de usuario quedará bloqueada si se produce un cierto número de intentos fallidos de inicio de sesión dentro de un intervalo de tiempo especificado. Las cuentas bloqueadas no pueden utilizarse para iniciar sesiones. Una cuenta bloqueada continuará bloqueada hasta que un administrador la desbloquee o hasta que transcurra un intervalo de tiempo determinado. De forma predeterminada, el bloqueo de cuentas está desactivado.

La característica de bloqueo de cuentas no está disponible en Windows NT versión 3.1 ni en LAN Manager versión 2.x.

Existen cuatro parámetros relacionados con las contraseñas que se definen en el cuadro de diálogo Plan de cuentas.

Parámetro

Duración máxima de la contraseña: Intervalo de tiempo que puede utilizarse una contraseña antes de que el sistema obligue a cambiarla.



Duración mínima de la contraseña: Intervalo de tiempo que debe usarse una contraseña antes de que el usuario pueda cambiarla. Si selecciona la opción Permitir cambios inmediatamente, deberá seleccionar la opción "**No guardar historia de contraseñas**" bajo **Historia de contraseña**.

Longitud mínima de la contraseña: Número mínimo de caracteres que puede contener una contraseña.

Historia de contraseña: Número de contraseñas diferentes que debe utilizar una cuenta de usuario antes de poder reutilizar una contraseña antigua. Si indica un valor en este campo (por ejemplo, Recordar 4 contraseñas), entonces en Duración mínima de la contraseña deberá especificar un valor (por ejemplo, Permitir cambios en 7 días).

Si selecciona Cuenta bloqueada, también deberá establecer los parámetros siguientes.

Parámetro Significado.

Bloquear después de: Número de intentos fallidos de inicio de sesión que provocan el bloqueo de la cuenta. Los valores posibles son de 1 a 999.

Restablecer cuenta después de: Número máximo de minutos que pueden transcurrir entre dos intentos de inicio de sesión incorrectos. Los valores posibles son de 1 a 99999.Por ejemplo, si en Bloquear después de se especifican 5 intentos de inicio de sesión incorrectos y en Restablecer cuenta después de se indican 30 minutos, 5 intentos fallidos a

intervalos de 29 minutos bloquean la cuenta.

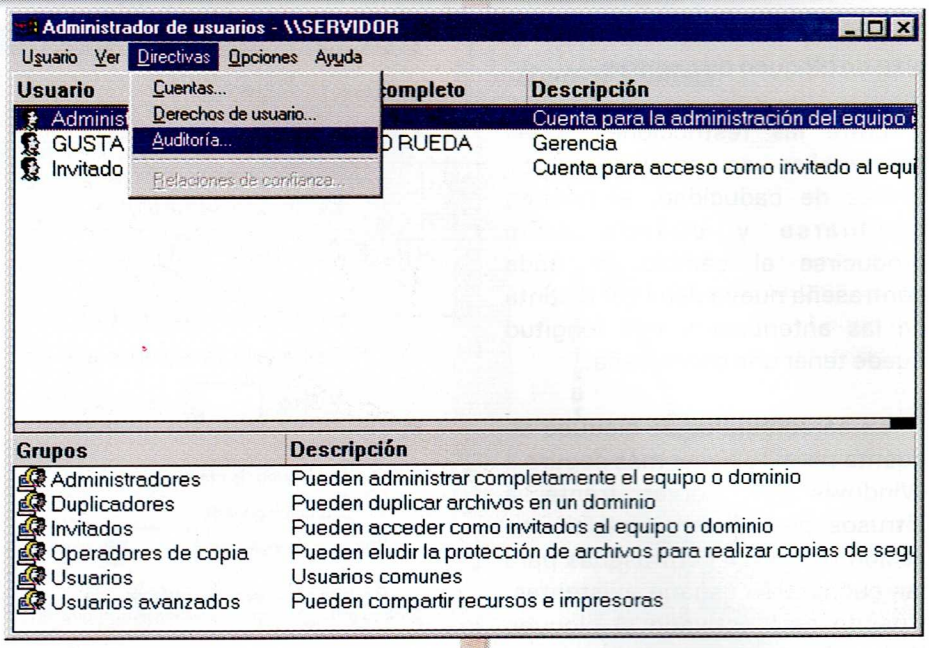
Duración del bloqueo: Seleccione **Para siempre** para que las cuentas bloqueadas continúen así hasta que un administrador las desbloquee. Seleccione Duración y escriba un número para que las cuentas permanezcan bloqueadas el número de minutos especificado.

La opción **Desconectar del servidor a los usuarios remotos cuando termine la hora de conexión** interactúa con las horas de sesión definidas para una cuenta de usuario. Si la opción está seleccionada, se cerrarán todas las conexiones con servidores del dominio de las cuentas de usuario que excedan el tiempo establecido en el cuadro de diálogo Horas de la sesión. El usuario recibe un mensaje de advertencia algunos minutos antes del final de las horas de sesión.

Si esta opción no está activada, no se desconectará el usuario una vez alcanzadas las Horas de sesión, pero el usuario no podrá establecer nuevas conexiones y recibirá un mensaje de advertencia cada 10 minutos.

Cuando está seleccionada la opción, los usuarios deben iniciar la sesión para cambiar la contraseña, los usuarios no pueden cambiar su propia contraseña una vez cadu-cada y necesitan la ayuda de un administrador. Cuando esta opción no está seleccionada, los usuarios pueden cambiar sus propias contraseñas cuando caducan sin ayuda de un administrador.

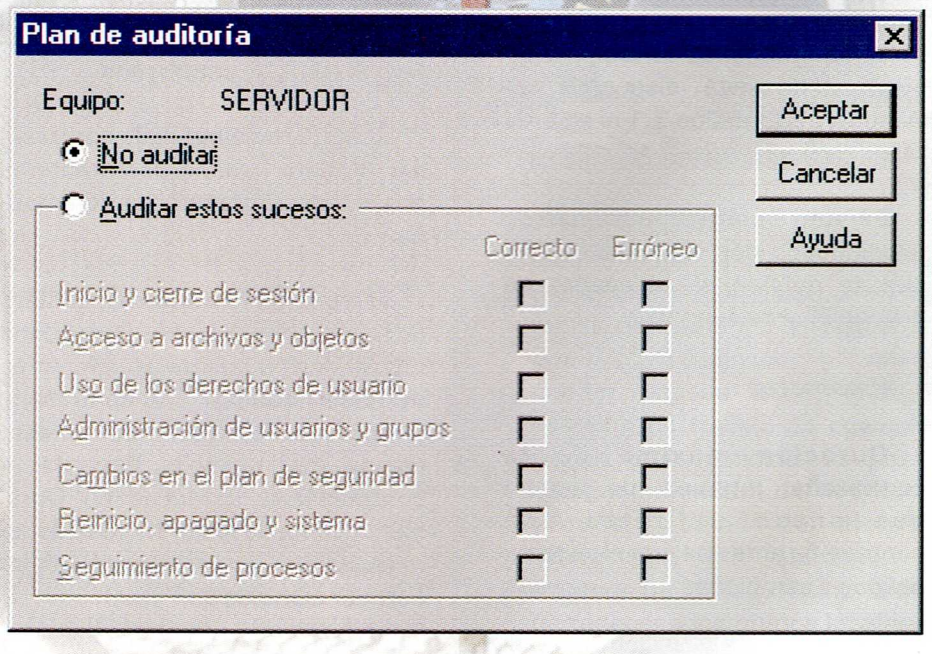
Los cambios en el plan de cuentas afectan a los usuarios del computador del dominio a partir del siguiente inicio de sesión.



Configuración del Plan de Auditoría.

Mediante la auditoría es posible hacer un seguimiento de determinadas actividades de los usuarios. En un controlador de dominio, el Plan de auditoría determina la cantidad y tipo de información de seguridad que registra Windows NT Server para todos los controladores del dominio. En las estaciones de trabajo y servidores miembros, el Plan de auditoría determina la cantidad y el tipo de información de seguridad que se registra en cada computador individual.

Windows NT puede registrar diversos tipos de sucesos, desde los que afectan a todo el sistema, como el inicio de sesión de un usuario, hasta los intentos por



CODESIS COMERCIALIZADORA EDITORIAL T. SISTEMAS LTDA.

parte de un usuario de leer un archivo determinado. Es posible registrar tanto las acciones que tienen éxito como las que fracasan.

Utilice el Plan de auditoría para seleccionar el tipo de sucesos de seguridad que deben registrarse. Cuando se produzca un suceso del tipo indicado, se agrega una entrada al registro de seguridad del computador. Utilice el **Visor de sucesos**, dentro de las **Herramientas administrativas** del menú **Inicio**, para examinar el registro de seguridad.

Definir la auditoría de archivos, directorios e impresoras es un proceso que consta de dos etapas.

Una vez activada la auditoría en el dominio y seleccionados los sucesos que se van a registrar, puede aplicar la auditoría a archivos, a directorios y a impresoras mediante la ficha **Seguridad** de la hoja de propiedades del objeto correspondiente.

Al administrar dominios, el Plan de auditoría se aplica al registro de seguridad del controlador principal del y al de reserva, ya que todos ellos comparten el mismo Plan de auditoría. Al administrar el computador con Windows NT Workstation o computadores con Windows NT Server que funcionen como servidores miembros, el plan sólo se aplica al registro de seguridad del computador individual.

La siguiente lista describe los tipos de sucesos que pueden registrarse.

Tipo de Suceso.

Inicio y cierre de sesión: Un usuario ha iniciado o terminado una sesión, o ha establecido una cone-xión de red.

Acceso a archivos y objetos: Un usuario ha abierto un directorio o un archivo elegido para auditoría en el Administrador de archivos, o ha enviado un trabajo de impresión a una impresora elegida para auditoría en el Administrador de impresión.

Uso de los derechos de usuario: Un usuario ha utilizado un derecho de usuario (excepto los relacionados con el inicio y fin de sesión).

Administración de usuarios y grupos: Se ha creado, modificado o eliminado una cuenta de usuario o de grupo. Se ha cambiado el nombre de una cuenta de usuario, se ha activado o desactivado, o se ha establecido o cambiado su contraseña.

Cambios en el plan de seguridad: Se ha efectuado un cambio en el Plan de derechos de usuario, en el de auditoría o en el de relaciones de confianza.

Reinicio, apagado y sistema: Un usuario ha reiniciado o apagado el computador, o se ha producido un suceso que afecta a la seguridad del sistema o al registro de seguridad.

Seguimiento de procesos: Estos sucesos proporcionan información de seguimiento detallada sobre sucesos tales como la activación de programas, algunas formas de duplicación de identificadores, accesos indirectos a objetos y salida de procesos.

Puesto que el tamaño del registro de seguridad es limitado, seleccione cuidadosamente los sucesos que se van a auditar y considere el espacio de disco que desea dedicar al registro de seguridad. El tamaño máximo del registro de seguridad se define en el **Visor de sucesos**.

Administración de Relaciones de Confianza.

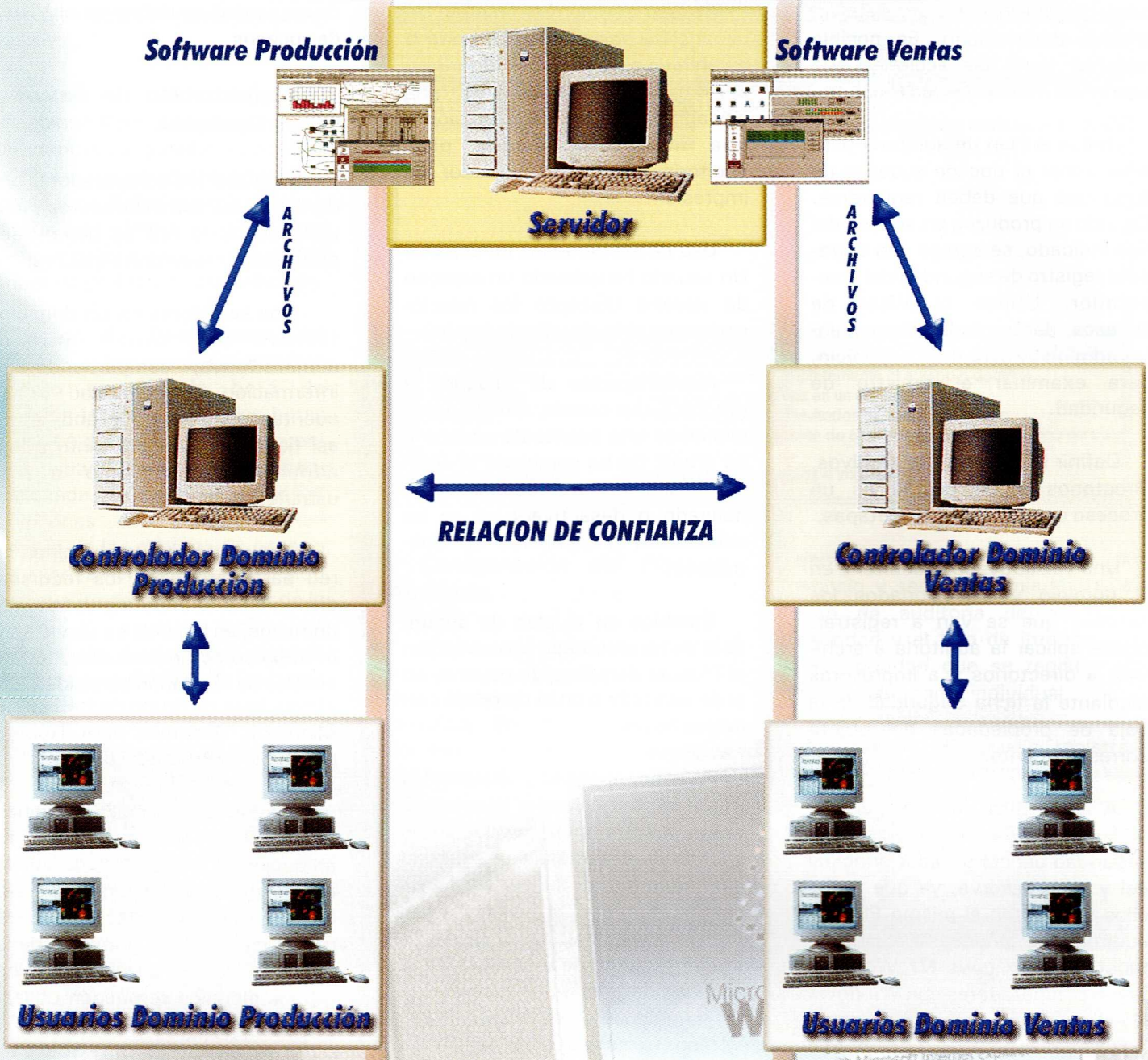
Al agrupar los computadores en dominios, los administradores y los usuarios de la red se benefician principalmente en dos aspectos:

- Los servidores de un dominio forman una única unidad administrativa, compartiendo la información de seguridad y de cuentas de usuario, y ahorrando así tiempo y esfuerzo tanto a los administradores como a los usuarios.

- Los usuarios que examinan la red para determinar los recursos disponibles la ven agrupada en dominios, en lugar de en servidores e impresoras individuales. (Esta ventaja de los dominios es idéntica al concepto de grupo de trabajo de Microsoft Windows para Trabajo en Grupo y Windows 95).

Las relaciones de confianza llevan las ventajas de la administración centralizada desde el nivel de dominios al nivel de red. Estableciendo relaciones de confianza entre los dominios de la red, las cuentas de usuario y los grupos globales se pueden utilizar en dominios distintos de aquél en el que se encuentran. Sólo es necesario crear una vez cada cuenta de usuario y, además, al permitir los servicios de directorio la sincronización de todos los datos de seguridad de la base de datos de directorio, es posible dotar a las cuentas de acceso a cualquier computador de la red, y no sólo a los computadores de un dominio.

Las relaciones de confianza sólo pueden crearse entre dominios de



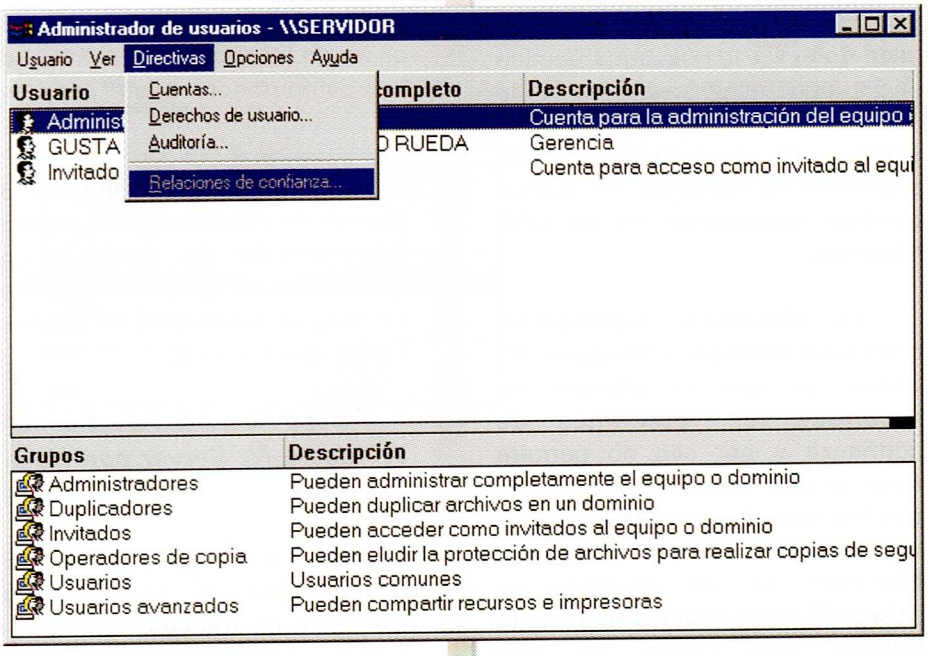
Windows NT Server. Al administrar servidores miembros, computadores con Windows NT Workstation o un dominio de LAN Manager 2.x, el comando **Relaciones de confianza** no está disponible.

El diagrama siguiente ilustra una relación de confianza entre dos dominios que contienen tanto recursos como cuentas.

Nota: Las flechas de los diagramas que representan relaciones de confianza siempre apuntan desde los recursos que pueden utilizarse hacia las cuentas en las que se confía para que los utilicen.

En el diagrama anterior, las cuentas de usuario del dominio Ventas pueden utilizar recursos del dominio Producción. El efecto de esta relación de confianza es que los usuarios de Ventas pueden iniciar una sesión en su dominio y recibir acceso a los servidores del dominio Producción, y además pueden hacerlo desde cualquier estación de trabajo de cualquiera de los dos dominios. Es posible agregar usuarios de Ventas a grupos locales del dominio Producción. Sin embargo, los usuarios de Producción no pueden pertenecer a los grupos locales del

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.



dominio Ventas, iniciar sesiones en el dominio Producción desde estaciones de trabajo de Ventas ni conectar con servidores del dominio Ventas.

Una situación habitual adecuada para una relación de confianza unidireccional es un domino que sólo contiene cuentas y en el que confían uno o más dominios de recursos. En esa configuración de confianza, se confía en todas las cuentas para que utilicen todos los recursos.

Creación de una Relación de Confianza entre dos Dominios.

Para crear relaciones de confianza se utiliza el comando **Relaciones de confianza** del menú **Directivas del Administrador de usuarios para dominios**.

La creación de una relación de confianza unidireccional tiene dos etapas: en primer lugar, un dominio (aquél en el que se va a confiar) debe agregar un segundo dominio (el dominio que va a confiar) a la lista de los dominios que confían en él; en segundo lugar, el dominio que confía debe agregar el dominio en el que va a confiar a la lista de los dominios en los que confía. Como la relación de confianza aún no se ha establecido, es posible que sean dos administradores distintos quienes tengan que realizar estos dos pasos.

Es mejor establecer primero la relación Autorizados a confiar en este dominio y después la relación Dominios en los que se confía. Al seguir este orden, la contraseña establecida para configurar la relación de confianza puede comprobarse inmediatamente la primera vez que se utiliza la relación.

Quitar una Relación de Confianza entre dos Dominios.

Para quitar una relación de confianza es necesario quitar sus dos partes. En el dominio de confianza, quite el dominio en el que se confía. En el dominio en el que se confía, quite el dominio de confianza.

INTEGRACIÓN DE WINDOWS NT SERVER CON SISTEMAS EXISTENTES.

Microsoft Windows NT Server se integra bien con sistemas de red ya existentes, como por ejemplo Novell NetWare y LAN Manager. Windows NT Server ofrece el software necesario para establecer comunicaciones entre los computadores con Windows NT Server y otros computadores y recursos de la red. Sin embargo, debido a la diversidad de protocolos y servicios, es necesario conocer los requisitos de la organización antes de instalar Windows NT Server.

Para que dos computadores se comuniquen a través de una red, deben compartir al menos un protocolo de red. Antes de instalar Windows NT Server debe conocer los requisitos de su organización.

Cuentas de Usuario Locales.

Si la red tiene actualmente servidores con sistemas operativos distintos de Windows NT, como por ejemplo LAN Manager 2.x, Novell NetWare o IBM LAN Server, puede utilizar cuentas de usuario locales para facilitar el acceso a la red de usuarios de estos sistemas y usuarios de cuentas de dominios de Windows NT Server.

Las cuentas de usuario locales no pueden emplearse para iniciar sesiones interactivamente en un computador con Windows NT Server como servidor miembro o con Windows NT Workstation, pero en la mayoría de los demás aspectos se asemejan a las cuentas de usuario habituales: Pueden conectar con computadores que ejecuten Windows NT Server o Windows NT Workstation

a través de la red, pueden agregarse a grupos globales y locales, y pueden recibir permisos sobre recursos y derechos de usuario. La única excepción es que las cuentas locales creadas en un dominio no pueden utilizarse en los dominios que confíen en él. Su uso está limitado a un único dominio.

Las cuentas locales se crean y utilizan en un dominio en dos tipos de situaciones:

- Para permitir a los usuarios de otros dominios de Windows NT Server conectar con los servidores LAN Manager 2.x del dominio

- Para permitir a los usuarios cuyas cuentas de usuario se encuentran en dominios en los que no se confía, o que no funcionan con Windows NT Server, conectar con computadores que ejecutan Windows NT Server o Windows NT Workstation en este dominio.

Las cuentas locales se crean de la misma forma que las cuentas de usuario normales, excepto en que al hacerlo se debe usar el botón **Cuenta del cuadro** de diálogo **Usuario nuevo** del Administrador de usuarios para dominios, indicando así que se trata de una cuenta local.

Funcionamiento de Windows Nt Server con Lan Manager.

Windows NT Server mantiene la compatibilidad con los servidores LAN Manager al tiempo que amplía y mejora el conjunto de características de éstos. Por ejemplo, Windows NT Server aprovecha el modelo de dominios de LAN Manager, pero simplifica la administración de los dominios. En lugar de cuatro tipos de servidores, sólo hay tres; en lugar de ser necesaria una cuenta de usuario en cada dominio, los usuarios pueden iniciar una única sesión teniendo por ámbito toda la red. De forma similar, las características de seguridad de Windows NT Server también aprovechan las de LAN Manager.

Una diferencia significativa entre LAN Manager y Windows NT Server es que el primero no reconoce las relaciones de confianza y por ello no permite tener grupos locales. Para permitir que los usuarios tengan acceso a los recursos de los servidores LAN Manager de un dominio es necesario crear cuentas de usuario locales para todos los que necesiten utilizar los recursos.

Las estaciones de trabajo no requieren un software actualizado para la transición de un dominio de LAN Manager a uno de Windows NT Server. Sin embargo, para asegurar que el dominio correcto valida las peticiones de inicio de sesión, los clientes MS-DOS LAN Manager deben funcionar con LAN Manager versión 2.1 o posterior. Cuando los clientes trabajan con software anterior a LAN Manager 2.1, el nombre del dominio no se transfiere, sino que se difunde por la red hasta que un servidor reconoce el nombre de inicio de sesión. Con ello no sólo se afecta al rendimiento, sino que es posible que un usuario tenga cuentas en varios dominios y que no sea validado por el controlador de dominio correcto.

Administración de Servidores Microsoft Lan Manager.

Al administrar servidores Microsoft LAN Manager 2.1 o posterior, algunas funciones del Administrador de servidores no estarán disponibles o funcionarán de modo ligeramente distinto al de los computadores con Windows NT.

Al administrar un dominio de Microsoft LAN Manager 2.x con el Administrador de servidores no estarán disponibles los comandos Servidores, Estaciones de trabajo y Todos del menú Ver.

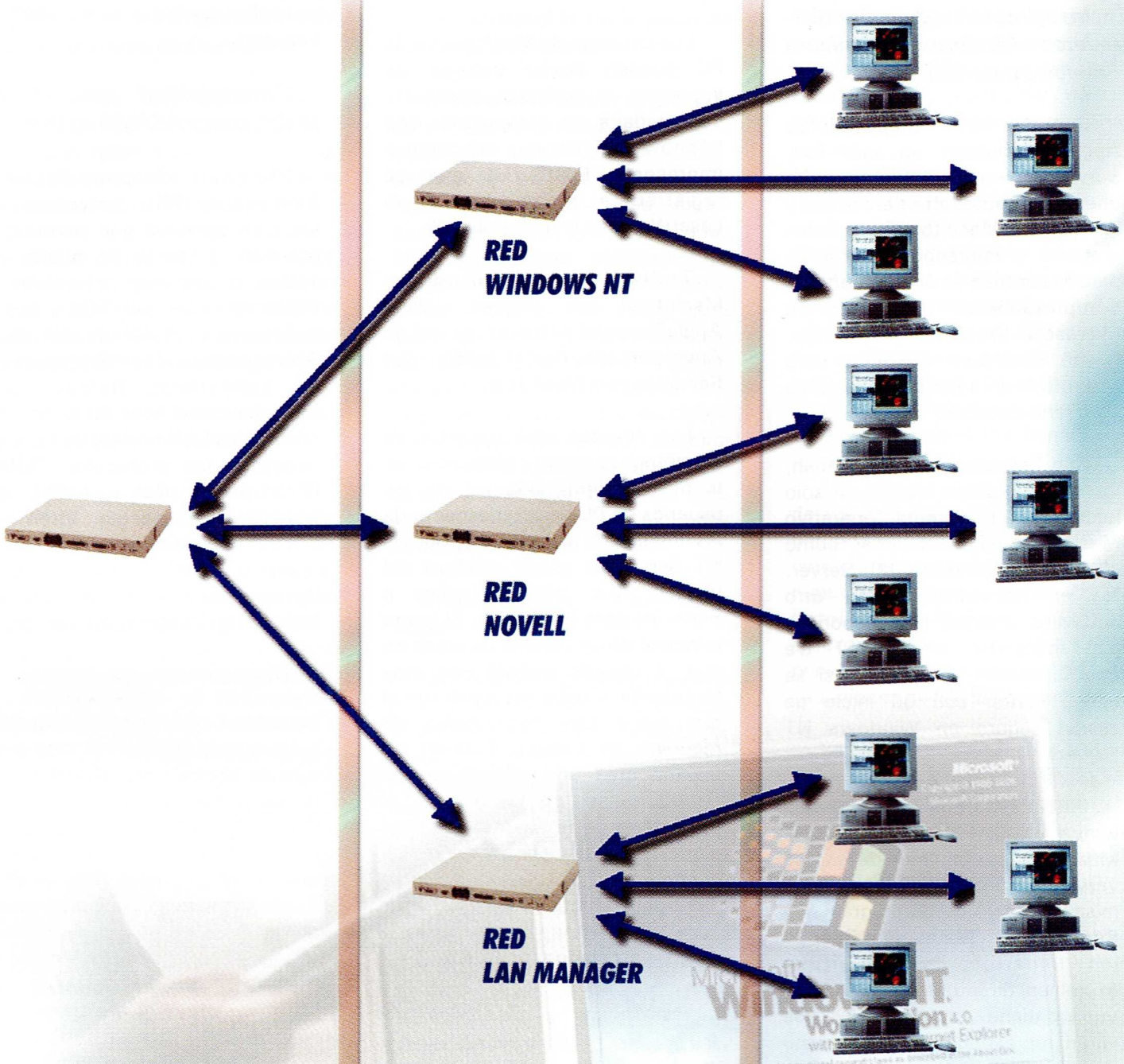
Funcionamiento de Windows Nt Server con Novell Netware.

Windows NT Server proporciona el software de protocolo de transporte necesario para comunicarse con computadores NetWare, y el Servicio de puerta de enlace o Gateway que permite a los servidores y estaciones de trabajo de un dominio de Windows NT Server utilizar los recursos de los servidores de red NetWare, y la posibilidad de migrar de NetWare a Windows NT Server.

Windows NT Workstation y Windows NT Server incluyen software cliente que permite conexiones con servidores NetWare. Con el Servicio de cliente para NetWare de Windows NT Workstation y el Servicio de puerta de enlace o Gateway para NetWare de Windows NT Server, los usuarios pueden utilizar los recursos de archivos y de impresión de los servidores NetWare 2.x a 4.x.

Además de actuar como software cliente para NetWare, el Servicio de puerta de enlace o Gateway permite el acceso a los servidores NetWare de computadores clientes Microsoft de la red que no cuentan con software cliente para NetWare. Los computadores sin software

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.



cliente para NetWare pueden conectar con los recursos de NetWare como si se encontrasen en un computador con Windows NT Server. Los administradores pueden controlar qué usuarios pueden establecer un Gateway y qué recursos pueden compartirse a través del mismo

.

Además, Servicios de archivos e impresión para NetWare permite que un computador con Windows NT Server funcione como servidor de archivos y de impresión compatible con NetWare 3.12. Los computadores con el software de cliente NetWare pueden utilizar los recursos de archivos e impresión y las aplicaciones de servidor avanzadas del mismo equipo de propósito múltiple con Windows NT Server. Esta característica permite a los usuarios de NetWare integrar servidores con Windows NT Server sin incurrir en los elevados costos que supone reconfigurar sus escritorios y redes.

Integración de Computadores Macintosh Mediante Servicios para Macintosh.

Cuando hay computadores Apple Macintosh en una red, Servicios para Macintosh permite que los computadores personales y los clientes Macintosh compartan archivos e impresoras. Servicios para Macintosh es un componente completamente integrado en Microsoft Windows NT Server. Puede configurar Servicios para Macintosh durante la instalación o agregarlo después.

Con Servicios para Macintosh, los computadores Macintosh sólo necesitan el sistema operativo Macintosh para funcionar como clientes de Windows NT Server. No es necesario ningún otro software, aunque hay disponible un módulo opcional de autentificación de usuarios si se desea contar con un inicio de sesión seguro en Windows NT Server.

En el caso de aplicaciones que tienen versiones para PC y para Macintosh, los usuarios de las dos versiones pueden trabajar sobre el mismo archivo de datos gracias a Servicios para Macintosh. Cuando los usuarios de Macintosh examinen directorios del servidor que contiene estos archivos, los verán representados por el icono correspondiente. Por ejemplo, si un usuario utiliza una versión para PC de Microsoft Excel, puede crear un archivo de hoja de cálculo y almacenarlo en el servidor dentro de un directorio compartido, configurado también como volumen accesible para Macintosh. Un usuario de Macintosh que abra esa carpeta verá el archivo representado por el icono que en Macintosh representa a una hoja de cálculo de Microsoft Excel.

Los usuarios de Macintosh y de PC pueden enviar trabajos de impresión a cualquier impresora conectada a un computador con Windows NT Server, así como a impresoras PostScript que se registren a sí mismas como LaserWriter en la red AppleTalk.

Todos los computadores Macintosh que pueden utilizar AppleShare (el software de red de Apple para Macintosh) pueden usar Servicios para Macintosh.

Las cuentas para usuarios de Macintosh se crean y almacenan de la misma forma que las de los usuarios de PC. Hay un aspecto de las cuentas de usuario de Windows NT Server, el grupo principal del usuario, que sólo se aplica a Servicios para Macintosh. El grupo principal de un usuario es aquél en que el usuario trabaja con más frecuencia, y debe ser aquél con el que tenga más necesidades de recursos en común. Cuando un usuario crea una carpeta en un servidor, se convierte en el propietario de la misma. El grupo principal del propietario se configura como el grupo asociado a la carpeta. Tanto el administrador como el propietario pueden cambiar el grupo asociado a la carpeta.

Protocolos y Servicios de Red que Proporcionan Conectividad.

Además de software específico para interactuar con redes Novell NetWare y Microsoft LAN Manager, y para utilizar computadores cliente Apple Macintosh y MS-DOS en dominios de Windows NT, Windows NT Server ofrece los protocolos y servicios de red que permiten intercambiar información entre computadores basados en Windows NT Server y la mayoría de las redes, incluídas redes UNIX e Internet.

Conectividad con Hosts Mainframe y AS/400 de IBM.

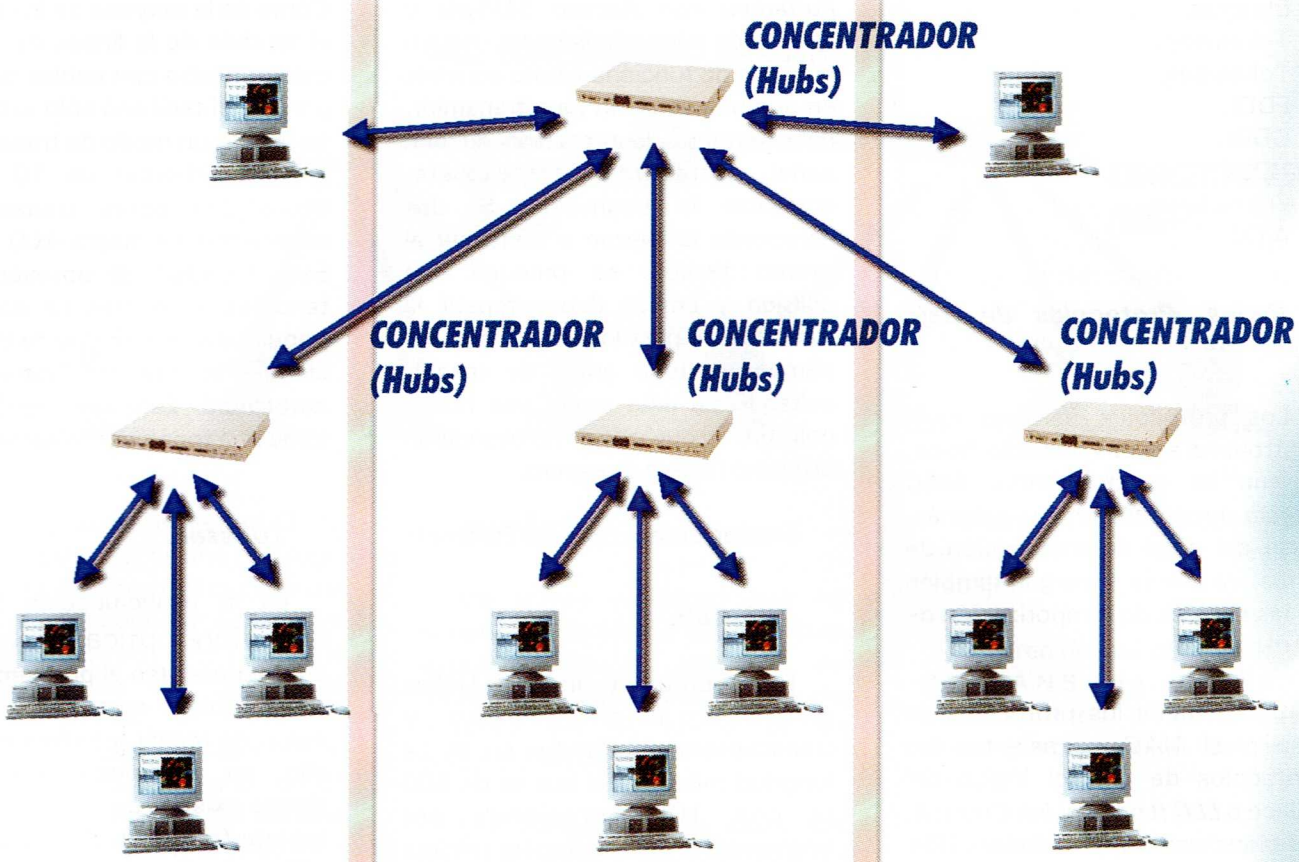
Microsoft System Network Architecture (SNA) Server es una solución opcional que permite la conexión a través de puerta de enlace o Gateway entre LAN o WAN formadas por PCs y hosts mainframe y AS/400 de IBM. SNA Server puede utilizar diversos tipos de conexiones físicas para conectar con el host. En el lado del cliente, las LAN o WAN de PC sólo necesitan los protocolos TCP/IP (Protocolo de control de transmisión/Protocolo Internet), IPX (Intercambio de paquetes entre redes) o NetBEUI para utilizar el Gateway de SNA, y todos ellos se incluyen en Windows NT Server.

Una puerta de enlace o Gateway de SNA elimina la necesidad de que se ejecute software de SNA en el host para administrar un puerto de comunicaciones por cada conexión de PC. En cambio, los computadores se conectan a través de una LAN al servidor SNA y éste requiere una única conexión al host.

Trabajo con Cuentas de Usuario y de Grupo.

Las cuentas de usuario y de grupo permiten que los usuarios participen en un dominio y tengan acceso a sus recursos. Los derechos y permisos asignados a las cuentas de usuario y a las cuentas de grupo proporcionan la cantidad de libertad necesaria y las restricciones que requieren los diferentes recursos de una organización.

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.



ESTRELLA JERARQUICA

Tokenring. Estos métodos y uno nuevo se describen a continuación:

Acceso Múltiple por detección de portadora / detección de colisiones (CSMA / CD): En este sistema las estaciones de trabajo conectadas a la red escuchan un tono de la portadora en el cable y envían la información en el momento que otras estaciones no están transmitiendo. El acceso múltiple significa que muchas estaciones comparten el mismo cable. Si dos o más estaciones detectan que la red esta preparada para transmitir, pueden intentar acceder a la red de forma simultanea provocando colisiones. Cada estación de trabajo debe entonces abandonar la operación y esperar una cierta cantidad de tiempo antes de empezar a retransmitir. El aumento del número de colisión pero se puede dividir en segmentos de para evitar la congestión.

- **Paso de testigo:** El testigo es un paquete de datos especial de las redes Token Ring, y la interfase de datos distribuida de fibra óptica (FDDI) que controla el acceso a la red.

Una estación de trabajo toma el control del paquete de datos testigo y tiene derecho de comunicar con la red. La diferencia con Ethernet es que las estaciones no acceden simultáneamente a la red. Solamente transmite una estación de trabajo que obtiene el paso de testigo disponible.

- **Método de acceso por prioridad de demandas:** Este es un sistema de acceso relativamente novedoso para Ethernet de 100 Mbits / Seg. Este devuelve la operación del acceso a la red a un concentrador central, en vez de confiar en las estaciones de trabajo individuales para determinar cuando deben acceder al cable. Las estaciones de trabajo piden permiso para transmitir en la base de datos a una prioridad y el concentrador transmite los datos de mayor jerarquía.

Protocolos de bajo nivel.

El protocolo de bajo nivel es, en cierto modo, la forma en que las señales se transmiten por el cable, transportando tanto datos como información y los procedimientos de control de uso del medio por las diferentes estaciones de trabajo. Los protocolos de bajo nivel más utilizados son:

Ethernet.
Token ring.
Token bus.
FDDI.
CDDI.
HDLC.
Frame Relay.
ATM.

Redes. Protocolos de bajo nivel.

Los protocolos de bajo nivel controlan el **acceso al medio físico**, lo que se conoce como ***MAC*** *(Media Access Control)* y, además, parte del nivel de transmisión de datos, ya que se encargan también de las señales de temporización de la transmisión.

Sobre todos los protocolos de bajo nivel *MAC*, se asientan los protocolos de control lógico del enlace o ***LLC*** *(Logical Link Control)*, definidos en el estándar IEEE 802.2.

Ethernet.

El protocolo de red Ethernet fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX Posteriormente, IEEE ha definido el estándar Ethernet 802.3. La forma de codificación difiere ligeramente en ambas definiciones.

Es el método de conexión más extendido en la actualidad.

La velocidad de transmisión de datos en Ethernet es de 10 Mbits/s.

En el caso del protocolo Ethernet/IEEE 802.3, el acceso al medio se controla con un sistema conocido como ***CSMA/CD*** *(Carrier Sense Multiple Access with Collision Detection, Detección de Portadora con Acceso Múltiple y Detección de Colisiones)*, cuyo principio de funcionamiento consiste en que una estación para transmitir, debe detectar la presencia de una señal portadora y, si existe, comienza la trasmisión. Si dos estaciones empiezan a transmitir al mismo tiempo, se produce una **colisión** y ambas deben repetir la transmisión, para lo cual esperan un tiempo aleatorio antes de repetir, evitando de este modo una nueva colisión, ya que ambas no escogerán el mismo tiempo de espera.

Existen cuatro tipos de Ethernet:

10base5.

Es la Ethernet original. Utiliza cable coaxial grueso y transceptores insertados en él. La longitud máxima del bus es de 500 m con 100 estaciones por segmento, a una distancia mínima de 2.5 m entre puntos de inserción de los transceptores.

10base2.

El costo de instalación del coaxial y los transceptores de las redes 10base5 las hacía prohibitivas para muchas empresas, lo cual indujo la utilización de un cable más delgado y, por tanto más barato, que además no necesitaba transceptores insertados en él. Por esto, también se le conoce **Ethernet fino** o ***cheaper-net*** *(red barata)*. La longitud máxima es de 185 metros y un máximo de 30 estaciones por segmento.

10baseT.

El costo del cable coaxial fino sigue siendo mayor que el del cable telefónico de pares trenzados. Como en la mayoría de los edificios el tendido de la líneas de teléfono estaba hecho con cables de cuatro pares y el teléfono sólo utiliza uno, se diseñó un modo de transmitir las señales Ethernet de 10 Mbits/s sobre dos pares trenzados en segmentos de hasta 100 metros. Esta facilidad de aprovechar los tendidos existentes ha dado gran popularidad a este tipo de Ethernet, siendo el más utilizado en la actualidad. Este tipo de Ethernet tiene una topología de estrella.

10baseF.

Es la especificación Ethernet sobre fibra óptica. Los cables de cobre presentan el problema de ser susceptibles tanto de producir como de recibir interferencias. Por ello, en entornos industriales o donde existen equipos sensibles a las interferencias, es muy útil poder utilizar la fibra. Normalmente, las redes Ethernet de fibra suelen tener una topología en estrella.

En la actualidad han surgido nuevas especificaciones basadas en Ethernet que permiten transmitir datos a mayor velocidad como son:

Switched Ethernet.

Esta especificación utiliza concentradores o hubs de red con canales de comunicación de alta velocidad en su interior, con una arquitectura similar a las centrales de teléfonos, que conmutan (*switch*) el tráfico entre las estaciones conectados a ellos. Esto permite que cada estación disponga de un canal de 10Mbits/s, en lugar de un único canal para todas ellas. La ventaja de esta especificación es que utiliza los mismos cables y tarjetas de red que el 10baseT, sustituyéndose sólo los concentradores.

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Ethernet de 100 Mbits/s (100baseX).

Esta especificación permite velocidades de transferencia de 100 Mbits/seg. sobre cables de pares trenzados, directamente desde cada estación. Requiere la sustitución de los concentradores y las tarjetas de red de las estaciones.

Token ring.

Las redes basadas en protocolos de **paso de testigo** (*token passing*) basan el control de acceso al medio en la posesión de un testigo. Éste es un paquete con un contenido especial que permite transmitir a la estación que lo tiene. Cuando ninguna estación necesita transmitir, el testigo va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el testigo a la siguiente.

Las redes de tipo token ring tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbits/s.

Existen redes token ring de 16 Mbits/s, pero no están definidas en ninguna especificación de IEEE.

Token bus.

Es una especificación de red basada en control de acceso al medio por paso de testigo con topología de bus.

FDDI.

Fiber Distributed Data Interface. Es una especificación de red sobre fibra óptica con topología de doble anillo, control de acceso al medio por paso de testigo y una velocidad de transmisión de 100 Mbits/s. Esta especificación estaba destinada a sustituir a la Ethernet pero el retraso en terminar las especificaciones por parte de los comités y los avances en otras tecnologías, principalmente Ethernet, la han relegado a unas pocas aplicaciones como interconexión de edificios.

CDDI.

Es una modificación de la especificación FDDI para permitir el uso de cables de cobre de la llamada **categoría cinco**, cables de alta calidad específicos para transmisión de datos, en lugar de fibra óptica.

HDLC.

Es la especificación de red utilizada principalmente en las transmisiones por líneas telefónicas para comunicaciones de datos, como pueden ser las líneas punto a punto y las redes públicas de conmutación de paquetes.

Frame Relay.

Frame Relay **(Paso de tramas)** puede ser tanto un servicio prestado por una compañía telefónica como una especificación de red privada. Este sistema de transmisión permite velocidades de 56 kbits/s, *n* x 64 kbits/s o 2 Mbits/s. El servicio se puede establecer con líneas punto a punto entre routers o por medio de una conexión con una red pública.

Un parámetro básico del servicio Frame Relay es el ***CIR*** *(Commited Information Rate, Tasa de información asegurada)*, el cual se utiliza para facturar las conexiones a redes públicas. Este valor se basa en la naturaleza aleatoria de la transmisión de datos, ya que no todas las estaciones transmiten al mismo tiempo, con lo cual, la suma de la capacidad, en bits/s, de los canales de cada una de ellas, puede ser superior a la capacidad de los canales de interconexión. Cada estación puede transmitir toda la información que permita el canal, pero, en caso de que la red se congestione, sólo podrá transmitir en principio la cantidad permitida por el CIR.

ATM.

Asynchronous Transfer Mode **(Modo de transferencia asíncrono)**. Es la especificación más reciente y con mayor futuro. Permite velocidades de a partir de 156 Mbits/s llegando a superar los 560 Mbits/s. Se basa en la transmisión de pequeños paquetes de datos de 56 bytes, con una mínima cabecera de dirección que son conmutados por equipos de muy alta velocidad. La gran ventaja de esta especificación es la capacidad que tiene para transmitir información sensible a los retardos como pueden ser voz o imágenes digitalizadas combinada con datos, gracias a la capacidad de marcar los paquetes como eliminables, para que los equipos de conmutación puedan decidir que paquetes transmitir en caso de congestión de la red.

Protocolos de red.

El protocolo de red determina el modo y organización de la información (tanto datos como controles) para su transmisión por el medio físico con el protocolo de bajo nivel. Los protocolos de red mas comunes son:

IPX/SPX.
DECnet.
X.25.

TCP/IP.
AppleTalk.
NetBEUI.

IPX/SPX.

Internet Packet eXchange/Sequenced Packet eXchange. Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red **Netware** de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

DECnet.

Es un protocolo de red propio de Digital Equipement Corporation (DEC), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y sus compatibles. Está muy extendido en el mundo académico.

Uno de sus componentes, **LAT** (*Local Area Transport*, transporte de área local), se utiliza para conectar periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.

X.25.

Es un protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

TCP/IP.

Este no es un protocolo, sino un conjunto de protocolos, que toma su nombre de los dos más conocidos: **TCP** (*Transmission Control Protocol*, protocolo de control de transmisión) e **IP** (*Internet Protocol*). Esta familia de protocolos es la base de la red Internet, la mayor red de ordenadores del mundo. Por lo cual, se ha convertido en el más extendido.

AppleTalk.

Este protocolo está incluído en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Existen tres formas básicas de este protocolo:

LocalTalk.

Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida pero es adecuada para los servicios que en principio se requieren de ella, principalmente compartir impresoras.

Ethertalk.

Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita aplicaciones como la transferencia de ficheros.

Tokentalk.

Es la versión de Appletalk para redes Tokenring.

NetBEUI.

NetBIOS Extended User Interface (Interfaz de usuario extendido para NetBIOS). Es la versión de Microsoft del **NetBIOS** (Network Basic Input/Output System, sistema básico de entrada/salida de red), que es el sistema de enlazar el *software* y el *hardware* de red en los PCs. Este protocolo es la base de la red de Microsoft Windows para Trabajo en Grupo.

El modelo OSI.

El modelo OSI (Open System Interconection) es utilizado por prácticamente la totalidad de las redes del mundo. Este modelo fue creado por el ISO (Organización Internacional de Normalización), y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas. Esta clasificación permite que cada protocolo se desarrolle con una finalidad determinada, lo cual simplifica el proceso de desarrollo e implementación. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores. Los siete niveles del modelo OSI son los siguientes:

Aplicación: El nivel de aplicación es el destino final de los datos donde se proporcionan los servicios al usuario.

Presentación: Se convierten e interpretan los datos que se utilizarán en el nivel de aplicación.

Sesión: Encargado de ciertos aspectos de la comunicación como el control de los tiempos.

CODESIS COMERCIALIZADORA EDITORIAL Y SISTEMAS LTDA.

Técnico en Redes y Comunicaciones para Computadores

Test No. 4

Test de Evaluación

Establecimiento del Cumplimiento de logros

Esta evaluación ha sido elaborada por el editor, CODESIS LTDA, con el objetivo de que el lector establezca el cumplimiento de logros en el proceso de aprendizaje paso a paso del Curso Técnico en Redes y Comunicaciones para Computadores.
Se trata de 20 preguntas de respuestas concretas y en ocasiones algo extensas, sobre los temas tratados en el transcurso del presente fascículo.
El lector deberá resolver por escrito las que él considere son las respuestas correctas de esta evaluación.
Para obtener el Diploma deberá enviarnos las evaluaciones, todas al final de la obra, o una por una semanalmente a nuestra dirección: Av. 22 No 40-77 Of. 302 Santafé fe Bogotá o nuestro e-mail codesis@latino.net.co

SOFTWARE

1. Qué es sincronizar la base de datos de directorio?
2. Cuál es la diferencia entre sincronización parcial y total?
3. Explique cómo agregar una estación de trabajo o un servidor a un dominio?
4. Explique cómo eliminar un computador de un dominio?
5. Qué se debe hacer para cambiar el nombre de un computador de una estación de trabajo?
6. Qué es un plan de seguridad de un dominio?
7. Cómo se configura un plan de auditoría?
8. Qué es una relación de confianza?
9. Cómo se crea una relación de confianza entre dos dominios?
10. Con qué sistemas se puede integrar Windows NT Server?

HARDWARE

1. Describa las características de una topología en estrella.
2. Describa las características de una topología anillo en estrella.
3. Qué es inter redes?
4. Qué es una red de enlace central?
5. Qué son protocolos de bajo nivel?
6. Describa Ethernet.
7. Describa 10base T.
8. Describa Token Ring.
9. Describa protocolos de red.
10. Describa NetBEUI.

Técnico en Redes y Comunicaciones para Computadores

Hardware 1: Fascículo 10
Windows NT: Fascículo 20
Hardware 2: Fascículo 30
Novell 5: Fascículo 40

Contenido General de la Obra:

Software

Windows NT

- Glosario Fascículo 0
- Introducción a Windows NT
- Planificación e instalación de Windows NT Server
- Conociendo el entorno de Windows NT
- Usuarios
- Sistemas de archivos y directorios
- Ejecutar aplicaciones
- Seguridad
- Uso compartido de recursos
- Trabajo de Red
- Configuración de los componentes de la red
- Impresión
- Administración de Windows NT
- Administración de servicios de Impresión
- Utilidades y ordenes para usuarios
- Comunicaciones
- Conectividad con
- Netware
- TCP/IP
- Servicio de Acceso Remoto (RAS)
- Rendimiento
- Mantenimiento del sistema

Novell Netware 5.0

- Glosario (Fascículo 0)
- Introducción a Netware 5.0
- Planificación e instalación de Netware 5.0
- Instalación y administración de clientes
- Planificación de servicios de Netware 5.0
- Ordenes y utilidades de la consola
- Herramientas de administración Netware
- Administración de usuarios y objetos
- Creación y modificación de usuarios
- Asignación de derechos sobre archivos y directorios
- Administración del árbol NDS y particiones
- Administración del sistema de archivos
- Gestión de directorio y archivos
- Comandos para directorios y archivos
- Servicios de impresión en Netware y comandos
- Conexiones
- Menús de Netware
- Protección, copia y seguridad de datos
- Sistema de facturación Netware
- Herramientas y técnicas de Administración
- Comunicaciones

Hardware

- Glosario (Fascículo 0)
- Introducción
- Tipos de redes
- Componentes de una red básica
- Adaptadores
- Guía de cableado
- Modelo OSI
- Segmentos de red
- Hubs (Conectores)
- Repetidores
- Bridges
- Routers
- Switches de Redes
- Topología de redes
- Proyecto completo cableado estructurado
- Voz - datos - cableado horizontal - Cableado vertical
- Backbone

Comunicaciones

- Correo electrónico
- Modos de transmisión asincrónico, sincrónico
- Transmisión inalámbrica
- Sistema telefónico
- Satélites de
- comunicación
- Redes satelitales
- Intranet

DISTRIBUCION:

MEXICO:	DISTRIBUIDORA INTERMEX S.A. Teléfono: 230 95 00 (México D.F)
CHILE:	DISTRIBUIDORA ALFA Teléfono: 525 5599 (Santiago)
ARGENTINA:	DISTRIBUIDORA BERTRAN Teléfono: 4303 1870 (Buenos Aires)